(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－40097

(43)公開日　平成10年(1998)２月13日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　9/06	５５０		Ｇ０６Ｆ　9/06	５５０Ｚ	
11/30			11/30	Ｈ	
11/32			11/32	Ｋ	
11/34			11/34	Ｃ	

審査請求　未請求　請求項の数３　ＯＬ　（全９頁）

(21)出願番号　特願平8－189331

(22)出願日　平成８年(1996)７月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　久田　永子
東京都府中市東芝町１番地　株式会社東芝府中工場内

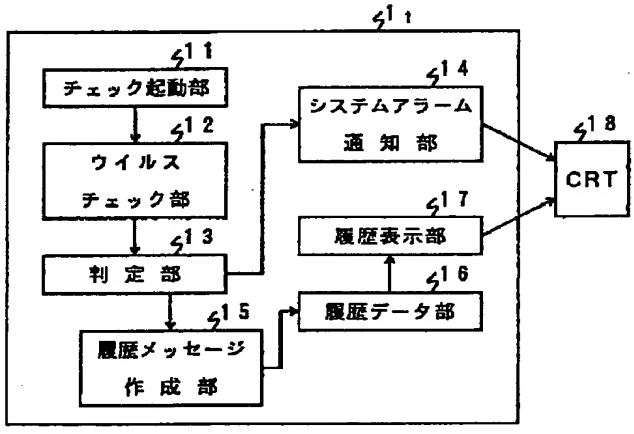
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　ウイルスチェック機能付計算機

(57)【要約】

【課題】　本発明は、定期的にウイルスチェックプログラムを起動させ、ウイルスを駆除し、ウイルス感染によるシステムへの悪影響の抑制を図る。

【解決手段】　ウイルスチェック手段(12)が、起動手段(11)から起動指令を受けたとき、コンピュータウイルスの検出及び駆除のためのウイルスチェック処理を実行し、データ送出手段(12)が、コンピュータウイルスが検出されたとき、ウイルス検出データを送出し、また、コンピュータウイルスが駆除されたとき、ウイルス駆除データを送出し、メッセージ出力手段(15,17)が、ウイルス検出データに基づいて、検出メッセージを作成及び出力し、また、ウイルス駆除データに基づいて、駆除メッセージを作成及び出力し、履歴データメモリ(16)では、ウイルス検出データ及びウイルス駆除データのうち、少なくともメッセージの内容が時系列的に記憶されるウイルスチェック機能付計算機。



1

【特許請求の範囲】
【請求項１】　他の計算機とネットワークを介して接続されたウイルスチェック機能付計算機において、
定期的に起動指令を発生する起動手段と、
前記起動手段から起動指令を受けたとき、コンピュータウイルスの検出及び駆除のためのウイルスチェック処理を実行するウイルスチェック手段と、
前記ウイルスチェック手段によりコンピュータウイルスが検出されたとき、ウイルス検出データを送出し、前記ウイルスチェック手段によりコンピュータウイルスが駆除されたとき、ウイルス駆除データを送出するデータ送出手段と、
前記データ送出手段から送出されたウイルス検出データに基づいて、検出メッセージを作成及び出力し、前記データ送出手段から送出されたウイルス駆除データに基づいて、駆除メッセージを作成及び出力するメッセージ出力手段と、
前記データ送出手段から送出されたウイルス検出データ及びウイルス駆除データのうち、少なくとも前記メッセージ出力手段にて作成される両メッセージの内容が時系列的に記憶される履歴データメモリとを備えたことを特徴とするウイルスチェック機能付計算機。
【請求項２】　請求項１に記載のウイルスチェック機能付計算機において、
前記データ送出手段からウイルス検出データが送出されたとき、自己の計算機本体と前記ネットワークとの接続を切り離すウイルス隔離手段を備え、
前記メッセージ出力手段では、前記ウイルス隔離手段により接続が切り離されたとき、隔離メッセージを作成及び出力し、
前記履歴データメモリでは、このメッセージ出力手段にて作成される隔離メッセージの内容が時系列的に記憶されることを特徴とするウイルスチェック機能付計算機。
【請求項３】　請求項１又は請求項２に記載のウイルスチェック機能付計算機において、
前記履歴データメモリでは、新たにソフトウェアがインストールされたとき、前記ソフトウェアの識別データが時系列的に記憶されることを特徴とするウイルスチェック機能付計算機。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータウイルスを検出及び駆除するためのウイルスチェック機能付計算機に関する。
【０００２】
【従来の技術】近年、計算機（以下、コンピュータという）の普及に伴い、他人のコンピュータに侵入して種々の誤動作を生じさせる、いわゆるコンピュータウイルスが発見されている。
【０００３】この種のコンピュータウイルス（以下、ウイルスという）は、感染により、比較的軽微な異常を起こすものから重大な故障を引き起こすものまで様々な種類があるが、軽微なものであっても不測の事態を生じさせる恐れがあり、極力駆除する必要がある。

2

【０００４】例えば、プロセス制御システム内の監視操作用コンピュータでは、ウイルスに感染した場合、ネットワークを介してプロセスに異常を発生させる可能性があるため、徹底した駆除が求められている。そこで、係る監視操作用コンピュータでは、一般のパーソナルコンピュータ用ウイルスチェックプログラムを用いたウイルスチェック機能が付加されており、操作者の操作により、任意の時期にウイルスチェックプログラムが起動され、ウイルス感染の有無がチェックされている。なお、任意の時期とは、例えばソフトウェアインストール時である。
【０００５】一方、ウイルスが発見された場合、操作者の操作により、その監視操作用コンピュータをネットワークから切り離し、他の監視操作用コンピュータへの感染を防止している。
【０００６】
【発明が解決しようとする課題】しかしながら以上のようなウイルスチェック機能付計算機では、操作者がウイルスチェックの実行時期を判断し、その都度、ウイルスチェックプログラムを起動させる必要があるため、ウイルス感染の有無を適切に監視することが困難である。
【０００７】例えば、判断されたウイルスチェックの実行時期が不適切な場合、ウイルスの発見が遅れ、プロセス制御システムに悪影響を与える可能性がある。また、ウイルスが発見されても、操作者の操作により、監視操作用コンピュータを切り離すため、ウイルス感染した監視操作用コンピュータの隔離が遅れ、同様にプロセス制御システムに悪影響を与える可能性がある。
【０００８】また、ウイルスが発見されても、ウイルスの感染時期や感染源の特定が極めて困難であるため、同一ソフトウェアの使用による他の監視操作用コンピュータあるいは他のプロセス制御システム等への感染の拡大を防止できない問題がある。
【０００９】本発明は上記実情を考慮してなされたもので、定期的にウイルスチェックプログラムを起動させ、ウイルスの駆除や感染したコンピュータの切り離しを実行することにより、ウイルス感染によるシステムへの悪影響を最小限に抑制し得るウイルスチェック機能付計算機を提供することを目的とする。
【００１０】また、本発明の他の目的は、ウイルスチェックの履歴を管理することにより、ウイルスの感染源を特定でき、感染の拡大を阻止し得るウイルスチェック機能付計算機を提供することにある。
【００１１】
【課題を解決するための手段】請求項１に対応する発明は、他の計算機とネットワークを介して接続されたウイ

ルスチェック機能付計算機において、定期的に起動指令を発生する起動手段と、前記起動手段から起動指令を受けたとき、コンピュータウイルスの検出及び駆除のためのウイルスチェック処理を実行するウイルスチェック手段と、前記ウイルスチェック手段によりコンピュータウイルスが検出されたとき、ウイルス検出データを送出し、前記ウイルスチェック手段によりコンピュータウイルスが駆除されたとき、ウイルス駆除データを送出するデータ送出手段と、前記データ送出手段から送出されたウイルス検出データに基づいて、検出メッセージを作成及び出力し、前記データ送出手段から送出されたウイルス駆除データに基づいて、駆除メッセージを作成及び出力するメッセージ出力手段と、前記データ送出手段から送出されたウイルス検出データ及びウイルス駆除データのうち、少なくとも前記メッセージ出力手段にて作成される両メッセージの内容が時系列的に記憶される履歴データメモリとを備えたウイルスチェック機能付計算機である。

【００１２】また、請求項２に対応する発明は、請求項１に対応するウイルスチェック機能付計算機において、前記データ送出手段からウイルス検出データが送出されたとき、自己の計算機本体と前記ネットワークとの接続を切り離すウイルス隔離手段を備え、前記メッセージ出力手段では、前記ウイルス隔離手段により接続が切り離されたとき、隔離メッセージを作成及び出力し、前記履歴データメモリでは、このメッセージ出力手段にて作成される隔離メッセージの内容が時系列的に記憶されるウイルスチェック機能付計算機である。

【００１３】さらに、請求項３に対応する発明は、請求項１又は請求項２に対応するウイルスチェック機能付計算機において、前記履歴データメモリでは、新たにソフトウェアがインストールされたとき、前記ソフトウェアの識別データが時系列的に記憶されるウイルスチェック機能付計算機である。

（補足説明）次に、以上のようなウイルスチェック機能付計算機の内容を補足説明する。

【００１４】データ送出手段におけるウイルス検出データとしては、例えば、検出日時、ソフトウェア名、チェック方法及び結果などの項目が適宜使用可能である。同様に、ウイルス駆除データとしては、例えば、駆除日時、ソフトウェア名、駆除方法及び結果などの項目が適宜使用可能である。

【００１５】また、メッセージ出力手段における検出メッセージとしては、少なくとも検出日時及び検出した旨を含んで作成されるが、混乱防止の観点からソフトウェア名も含んだものが好ましい。

【００１６】同様に、駆除メッセージとしては、少なくとも駆除日時及び駆除した旨を含んで作成されるが、混乱防止の観点からソフトウェア名も含んだものが好ましい。また、これら検出及び駆除メッセージは、必ずしも全てを文字や文章とする必要はなく、例えば日時以外の箇所を任意の図記号やイメージシンボル、静止画又は動画等で出力してもよい。

【００１７】履歴データメモリの内容は、検出日時、ソフトウェア名、チェック方法及び結果などの項目からなるウイルス検出データと、駆除日時、ソフトウェア名、駆除方法及び結果などの項目からなるウイルス駆除データと、ネットワークからの切り離し日時及び切り離した旨の隔離メッセージと、新たにインストールされたソフトウェアに関してインストール日時、識別データ及び供給元などの項目からなるソフトウェアインストールデータとを包含可能であるが、各項目は適宜省略可能である。

（作用）従って、請求項１に対応する発明は以上のような手段を講じたことにより、起動手段が定期的に起動指令を発生し、ウイルスチェック手段が、起動手段から起動指令を受けたとき、コンピュータウイルスの検出及び駆除のためのウイルスチェック処理を実行し、データ送出手段が、ウイルスチェック手段によりコンピュータウイルスが検出されたとき、ウイルス検出データを送出し、また、ウイルスチェック手段によりコンピュータウイルスが駆除されたとき、ウイルス駆除データを送出し、メッセージ出力手段が、データ送出手段から送出されたウイルス検出データに基づいて、検出メッセージを作成及び出力し、また、データ送出手段から送出されたウイルス駆除データに基づいて、駆除メッセージを作成及び出力し、履歴データメモリでは、データ送出手段から送出されたウイルス検出データ及びウイルス駆除データのうち、少なくともメッセージ出力手段にて作成される両メッセージの内容が時系列的に記憶されるので、定期的にウイルスチェックプログラムを起動させ、ウイルスを駆除することにより、ウイルス感染によるシステムへの悪影響を最小限に抑制することができ、また、ウイルスチェックの履歴を管理することにより、ウイルスの感染源の特定を期待することができる。

【００１８】また、請求項２に対応する発明は、ウイルス隔離手段が、データ送出手段からウイルス検出データが送出されたとき、自己の計算機本体とネットワークとの接続を切り離し、メッセージ出力手段が、ウイルス隔離手段により接続が切り離されたとき、隔離メッセージを作成及び出力し、また、履歴データメモリでは、このメッセージ出力手段にて作成される隔離メッセージの内容が時系列的に記憶されるので、請求項１に対応する作用と同様の作用に加え、ウイルスの検出に対応してネットワークを切り離すので、システムへの悪影響を一層、最小限に抑制することができる。

【００１９】さらに、請求項３に対応する発明は、請求項１又は請求項２に対応する履歴データメモリでは、新たにソフトウェアがインストールされたとき、ソフトウェアの識別データが時系列的に記憶されるので、請求項

１又は請求項２に対応する作用と同様の作用に加え、ソフトウェアインストールの履歴とウイルスチェックの履歴とを比較対照することにより、ウイルスの感染源を特定することができ、もって、感染の拡大を阻止することができる。

【００２０】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

（第１の実施の形態）図１は本発明の第１の実施の形態に係る監視操作用コンピュータの属するプロセス制御システムの構成を示すブロック図であり、図２はこの監視操作用コンピュータの構成を示すブロック図である。図１に示すプロセス制御システムは、監視操作のためのｎ台の監視操作用コンピュータ1_1～1_nが、ネットワーク２を介して監視操作対象としてのｍ台のプロセスコントロールステーション3_1～3_mに接続され、対応するプロセスコントロールステーション3_iを介してセンサ等による監視や弁等の操作端の制御を実行している。なお、添字のｉは１～ｍまでの任意の数である。また、各監視操作用コンピュータでは、本発明に係るウイルスチェック機能が互いに同一構成をもつため、以下、監視操作用コンピュータ1_1を例に挙げて説明する。

【００２１】ここで、監視操作用コンピュータ1_1は、パーソナルコンピュータが使用可能であり、図２に示すように、チェック起動部１１、ウイルスチェック部１２、判定部１３、システムアラーム通知部１４、履歴メッセージ作成部１５、履歴データ部１６、履歴表示部１７及びＣＲＴ１８を備えている。

【００２２】チェック起動部１１は、定期的に起動指令を発生し、この起動指令をウイルスチェック部１２に与えることにより、ウイルスチェック部１２を定期的に起動する機能をもっている。

【００２３】ウイルスチェック部１２は、チェック起動部１１により起動可能に一般のパーソナルコンピュータ用ウイルスチェックプログラムを有し、チェック起動部１１により起動されたとき、現在実行中のソフトウェアに関してウイルスを検出する機能と、検出したウイルスを駆除する機能と、ウイルスを未検出のとき（ウイルスの無いとき）、ウイルス無しデータを判定部１３に送出する機能と、ウイルスを検出したとき、ウイルス検出データを判定部１３に送出する機能と、ウイルスを駆除したとき、ウイルス駆除データを判定部１３に送出する機能とを備えている。

【００２４】なお、ウイルス無しデータは、チェック日時、ソフトウェア名、複数のチェック方法及び結果（ウイルス無し）の項目をもっている。同様に、ウイルス検出データは、チェック日時、ソフトウェア名、複数のチェック方法及び結果（ウイルス有り）の項目をもっている。ここで、ウイルス検出データは、必ずしも全てのチェック方法にて結果が「ウイルス有り」であることを要せず、少なくとも１つのチェック方法にて結果を「ウイルス有り」とするものが該当する。

【００２５】また同様に、ウイルス駆除データは、駆除日時、ソフトウェア名、駆除方法及び結果（駆除済み）の項目をもっている。判定部１３は、ウイルスチェック部１２から送出されたウイルス検出データをシステムアラーム通知部１４に送出する機能と、ウイルスチェック部１２から送出されるウイルス無しデータ、ウイルス検出データ又はウイルス駆除データを夫々履歴メッセージ作成部１５に送出する機能とをもっている。

【００２６】システムアラーム通知部１４は、判定部１３から送出されるウイルス検出データに基づいて音声や画面表示によるアラームをスピーカ付のＣＲＴ１８等に実行するものである。

【００２７】履歴メッセージ作成部１５は、判定部１３から送出される各データに基づいて、履歴メッセージを作成し、作成した履歴メッセージを履歴表示部１７から読出し可能な履歴データ部１６に書込む機能と、履歴メッセージに含まれない内容のデータを履歴データ部１６に書込む機能とをもっている。

【００２８】履歴表示部１７は、適宜、履歴データ部１６内の履歴メッセージを読出すと共に、読出した履歴メッセージをＣＲＴ１８に表示させる機能をもっている。次に、このようなウイルスチェック機能付の監視操作用コンピュータの動作を説明する。

【００２９】チェック起動部１１は、定期的にウイルスチェック部１２を起動する。ウイルスチェック部１２は、起動されると、現在実行中のソフトウェアに関してウイルスの有無をチェックし、感染している場合にはウイルスを検出し、ウイルス検出データを判定部１３に与える。また、ウイルスチェック部１２は、検出したウイルスを駆除すると共に、ウイルス駆除データを判定部１３に与える。

【００３０】判定部１３は、このウイルス検出データをシステムアラーム通知部１４及び履歴メッセージ作成部１５に与える。また、判定部１３は、このウイルス駆除データを履歴メッセージ作成部１５に与える。

【００３１】システムアラーム通知部１４は、ウイルス検出データに基づいて音声や画面表示によるアラームをＣＲＴ１８等に実行する。履歴メッセージ作成部１５は、ウイルス検出データに基づいて、履歴メッセージＭ１を作成し、作成した履歴メッセージＭ１を履歴データ部１６に書込む。また同様に、履歴メッセージ作成部１５は、ウイルス駆除データに基づいて、履歴メッセージＭ２を作成し、作成した履歴メッセージＭ２を履歴データ部１６に書込む。

【００３２】履歴表示部１７は、適宜、履歴データ部１６内の履歴メッセージを読出すと共に、図３に示すように、読出した履歴メッセージＭ１をＣＲＴ１８に表示させる。また同様に、履歴表示部１７は、履歴メッセージ

Ｍ２を読出してＣＲＴ１８に表示させる。なお、履歴メッセージＭ１などでは、メッセージ文の任意性を示す観点から「検出」という語を用いずに同義の「発見」という語を用い、同様に、「コンピュータウイルス」という語を用いずに「ソフトウェアウイルス」の語を用いた。

【００３３】また、ウイルスチェック部１２にてウイルスが検出されないとき、ウイルス無しデータが判定部１３を介して履歴メッセージ作成部１５に与えられる。履歴メッセージ部は、このウイルス無しデータに基づいて、履歴メッセージＭ３を作成して履歴データ部１６に書込む。履歴表示部１７は、この履歴メッセージＭ３を読出してＣＲＴ１８に表示させる。

【００３４】上述したように第１の実施の形態によれば、チェック起動部１１が定期的に起動指令を発生し、ウイルスチェック部１２が、この起動指令を受けたとき、コンピュータウイルスの検出及び駆除のためのウイルスチェック処理を実行し、且つウイルスを検出したとき、ウイルス検出データを送出し、また、ウイルスを駆除したとき、ウイルス駆除データを送出し、履歴メッセージ作成部１５及び履歴表示部１７にてウイルス検出データに基づいて、検出時の履歴メッセージを作成及び出力し、また、ウイルス駆除データに基づいて、駆除時の履歴メッセージを作成及び出力し、履歴データ部１６では、ウイルスチェック部１２から送出されたウイルス検出データ及びウイルス駆除データのうち、履歴メッセージ作成部１５にて作成される両履歴メッセージの内容が時系列的に記憶されるので、定期的にウイルスチェックプログラムを起動させ、ウイルスを駆除することにより、ウイルス感染によるシステムへの悪影響を最小限に抑制することができ、また、ウイルスチェックの履歴を管理することにより、ウイルスの感染源の特定を期待することができる。

【００３５】具体的には例えば、定期的にウイルスチェックを実行することにより、ウイルス感染によるシステムへの悪影響が大きくなる前に、容易に対応することができる。

【００３６】また、ウイルスチェックの履歴が保存されるために、ウイルス発見の時期からの感染源の絞り込みが可能となり、他システムへのウイルス感染を防止することができる。

【００３７】さらに、ウイルス発見時に直ちにシステムアラームが操作者に通知されるため、迅速な対応を期待することができる。

（第２の実施の形態）次に、本発明の第２の実施の形態について図面を参照して説明する。

【００３８】図４は係る監視操作用コンピュータの構成を示すブロック図であり、図２と同一部分には同一符号を付し、機能の付加された部分にはａの添字を付して同一部分の詳しい説明を省略し、ここでは異なる部分についてのみ述べる。

【００３９】すなわち、本実施の形態に係るコンピュータは、第１の実施の形態に対し、ウイルス検出時のネットワークの切り離し機能を付加したものであって、具体的には図４に示すように、ネットワークの切り離し要求を送出する機能の付加された判定部１３ａと、ネットワークを切り離した旨のメッセージ作成機能の付加された履歴メッセージ作成部１５ａとを有し、さらに両者の間にネットワーク診断部１９を備えたものである。

【００４０】ここで、判定部１３は、前述した機能に加え、ウイルスを検出したときにその旨をネットワーク診断部１９に通知する機能をもっている。ネットワーク診断部１９は、判定部１３ａからウイルスを検出した旨を通知されると、自己の監視操作用コンピュータをネットワークから切り離すと共に、切り離した旨を履歴メッセージ作成部１５ａに通知する機能をもっている。

【００４１】履歴メッセージ作成部１５ａは、前述した機能に加え、ネットワーク診断部１９から受けた通知に基づいて、自己の監視操作用コンピュータがネットワークから切り離された旨の履歴メッセージを作成し、その履歴メッセージを履歴データ部１６に書込む機能をもっている。

【００４２】次に、このように構成された監視操作用コンピュータの動作を説明する。いま、前述同様に、ウイルスチェック部１２が定期的にウイルスチェックを実行し、ウイルスを検出した旨を判定部１３ａに通知したとする。

【００４３】判定部１３ａは、ウイルスチェック部１２から受けた通知に基づいて、ウイルスを検出した旨をシステムアラーム通知部１４、履歴メッセージ作成部１５ａ及びネットワーク診断部１９に通知する。

【００４４】システムアラーム通知部１４及び履歴メッセージ作成部１５ａは、この通知を前述同様に処理する。一方、ネットワーク診断部１９は、この通知に基づいて、自己の監視操作用コンピュータをネットワークから切り離すと共に、切り離した旨を履歴メッセージ作成部１５ａに通知する。

【００４５】履歴メッセージ作成部１５ａは、この通知に基づいて、自己の監視操作用コンピュータがネットワークから切り離された旨の履歴メッセージＭ４を作成し、その履歴メッセージＭ４を履歴データ部１６に書込む。

【００４６】これにより、図５に示すように、ネットワークから切り離された旨の履歴メッセージＭ４が履歴表示部１７によりＣＲＴ１８上に表示される。上述したように第２の実施の形態によれば、ネットワーク診断部１９が、ウイルス検出データが送出されたとき、自己の計算機本体とネットワークとの接続を切り離し、履歴メッセージ作成部１５及び履歴表示部１７では、接続が切り離されたとき、切り離し時の履歴メッセージを作成及び出力し、また、履歴データ部１６では、この切り離し時

の履歴メッセージの内容が時系列的に記憶されるので、第１の実施の形態の効果に加え、ウイルスの検出に対応してネットワークを切り離すので、システムへの悪影響を一層、最小限に抑制することができる。

（第３の実施の形態）次に、本発明の第３の実施の形態について図面を参照して説明する。

【００４７】図６は係る監視操作用コンピュータの構成を示すブロック図であり、図２と同一部分には同一符号を付し、機能の付加された部分にはｂの添字を付して同一部分の詳しい説明を省略し、ここでは異なる部分についてのみ述べる。

【００４８】すなわち、本実施の形態に係るコンピュータは、第１の実施の形態に対し、ウイルス感染源の特定を図るものであり、具体的には図６に示すように、ソフトウェアのインストールに対応してソフトウェアインストールの履歴データを履歴メッセージ作成部１５に与えるソフトウェアインストール部２０と、ソフトウェアインストール部２０から受けた履歴データに基づいてソフトウェアインストールの履歴メッセージを作成して履歴データ部１６に保存するという機能の付加された履歴メッセージ作成部１５ｂと、履歴データ部１６内のソフトウェアインストールの履歴とウイルス検出の履歴とを確認するという機能の付加された履歴表示部１７ｂとを備えている。

【００４９】なお、ソフトウェアインストールの履歴データとしては、ソフトウェアのインストール日時、ソフトウェアの識別データ及び供給元の項目を有しているが、供給元の項目は省略可能である。

【００５０】次に、このような監視機能付コンピュータの動作を説明する。いま、前述同様に、チェック起動部１１が定期的にウイルスチェック部１２を起動することにより、ウイルスチェック部１２にて定期的にウイルスチェックが実行されているとする。

【００５１】また、これに並行し、新たにソフトウェアが自己の監視操作用コンピュータにインストールされたとき、ソフトウェアインストール部２０がソフトウェアインストールの履歴データを履歴メッセージ作成部１５ｂに与える。

【００５２】履歴メッセージ作成部１５ｂは、このソフトウェアインストールの履歴データに基づいて、ソフトウェアインストールの履歴メッセージを作成し、作成した履歴メッセージを履歴データ部１６に書込む。

【００５３】一方、履歴表示部１７ｂは、適宜、履歴データ部１６内のウイルス検出・駆除に関する履歴メッセージをＣＲＴ１８に表示させると共に、ソフトウェアインストールの履歴メッセージを読出してＣＲＴ１８に表示させる。なお、この履歴メッセージは、例えば“１９９５年　１２月２５日　０９時４０分　　計算機１ｎからファイル名ｘｘｘ（のソフトウェア）をインストールしました。”というものである。

【００５４】これにより、ウイルス検出・駆除の両履歴メッセージＭ１，Ｍ２と、ソフトウェアインストールの履歴メッセージとが並列的に表示されるので、両者を比較対照することにより、ウイルス感染源を特定することができる。

【００５５】上述したように第３の実施の形態によれば、履歴データ部１６では、新たにソフトウェアがインストールされたとき、ソフトウェアのインストール日時、識別データ及び供給元が時系列的に記憶されるので、第１の実施の形態の効果に加え、ソフトウェアインストールの履歴とウイルスチェックの履歴とを比較対照することにより、ウイルスの感染源を特定することができ、もって、感染の拡大を阻止することができる。

（第４の実施の形態）次に、本発明の第４の実施の形態について図面を参照して説明する。

【００５６】図７は係る監視操作用コンピュータの構成を示すブロック図であり、図２、図４及び図６と同一部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分についてのみ述べる。

【００５７】すなわち、本実施の形態に係るコンピュータは、第１及び第２の実施の形態を互いに組合せたものであり、具体的には図７に示すように、図４に示すネットワーク診断部１９と、図６に示すソフトウェアインストール部２０とを備え、且つこれらの機能に対応した判定部１３ａ，履歴メッセージ作成部１５ａｂ，履歴表示部１５ｂを有している。なお、図７中、ａｂの添字は、第１の実施形態にて述べた機能に加え、第２の実施形態にて述べたａの機能と、第３の実施形態にて述べたｂの機能との両機能を備えたことを意味している。

【００５８】このような構成により、第１の実施の形態と同様に、定期的にウイルスチェックを行なってウイルス検出処理並びに駆除処理を実行してウイルス検出・駆除の両履歴メッセージＭ１，Ｍ２を表示処理し、第２の実施の形態と同様に、ウイルスを検出したときにネットワークからの切り離し処理及びその履歴メッセージＭ４の表示処理を実行し、第３の実施の形態と同様に、以上の処理に並行してソフトウェアインストールの履歴メッセージの表示処理を実行することができる。

【００５９】上述したように第４の実施の形態によれば、第１乃至第３の実施の形態の効果を同時に得ることができる。

（他の実施の形態）なお、上記第３及び第４の実施の形態では、感染源の特定のためにソフトウェアインストールの履歴データを管理する場合について説明したが、これに加え、感染源の特定のために外部ネットワークへのアクセス履歴、コンピュータ相互間の動作履歴、外部記憶媒体からのデータの読込み履歴などの感染の可能性のある動作の履歴データを適宜管理する構成としても、本発明を同様に実施して同様の効果を得ることができ、さらに、より一層感染源の特定を期待することができる。

【００６０】また、上記第１乃至第４の実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ，ＤＶＤなど）、半導体メモリなどの記憶媒体に格納して頒布することもできる。その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【００６１】

【発明の効果】以上説明したように請求項１の発明によれば、起動手段が定期的に起動指令を発生し、ウイルスチェック手段が、起動手段から起動指令を受けたとき、コンピュータウイルスの検出及び駆除のためのウイルスチェック処理を実行し、データ送出手段が、ウイルスチェック手段によりコンピュータウイルスが検出されたとき、ウイルス検出データを送出し、また、ウイルスチェック手段によりコンピュータウイルスが駆除されたとき、ウイルス駆除データを送出し、メッセージ出力手段が、データ送出手段から送出されたウイルス検出データに基づいて、検出メッセージを作成及び出力し、また、データ送出手段から送出されたウイルス駆除データに基づいて、駆除メッセージを作成及び出力し、履歴データメモリでは、データ送出手段から送出されたウイルス検出データ及びウイルス駆除データのうち、少なくともメッセージ出力手段にて作成される両メッセージの内容が時系列的に記憶されるので、定期的にウイルスチェックプログラムを起動させ、ウイルスを駆除することにより、ウイルス感染によるシステムへの悪影響を最小限に抑制することができ、また、ウイルスチェックの履歴を管理することにより、ウイルスの感染源の特定を期待できるウイルスチェック機能付計算機を提供できる。

【００６２】また、請求項２の発明によれば、ウイルス隔離手段が、データ送出手段からウイルス検出データが送出されたとき、自己の計算機本体とネットワークとの接続を切り離し、メッセージ出力手段が、ウイルス隔離手段により接続が切り離されたとき、隔離メッセージを作成及び出力し、また、履歴データメモリでは、このメッセージ出力手段にて作成される隔離メッセージの内容が時系列的に記憶されるので、請求項１の効果に加え、ウイルスの検出に対応してネットワークを切り離すので、システムへの悪影響を一層、最小限に抑制できるウイルスチェック機能付計算機を提供できる。

【００６３】さらに、請求項３の発明によれば、請求項１又は請求項２に対応する履歴データメモリでは、新たにソフトウェアがインストールされたとき、ソフトウェアの識別データが時系列的に記憶されるので、請求項１又は請求項２の効果に加え、ソフトウェアインストールの履歴とウイルスチェックの履歴とを比較対照することにより、ウイルスの感染源を特定することができ、もって、感染の拡大を阻止できるウイルスチェック機能付計算機を提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る監視操作用コンピュータの属するプロセス制御システムの構成を示すブロック図

【図２】同実施の形態における監視操作用コンピュータの構成を示すブロック図

【図３】同実施の形態における履歴メッセージの表示画面を示す模式図

【図４】本発明の第２の実施の形態に係る監視操作用コンピュータの構成を示すブロック図

【図５】同実施の形態における履歴メッセージの表示画面を示す模式図

【図６】本発明の第３の実施の形態に係る監視操作用コンピュータの構成を示すブロック図

【図７】本発明の第４の実施の形態に係る監視操作用コンピュータの構成を示すブロック図

【符号の説明】

1_1～1_n…監視操作用コンピュータ

２…ネットワーク

3_1～3_m，3_i…プロセスコントロールステーション

１１…チェック起動部

１２…ウイルスチェック部

１３，１３ａ…判定部

１４…システムアラーム通知部

１５，１５ａ，１５ｂ，１５ａｂ…履歴メッセージ作成部

１６…履歴データ部

１７，１７ｂ…履歴表示部

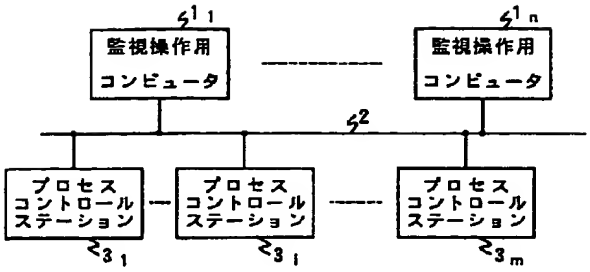
１８…ＣＲＴ

１９…ネットワーク診断部

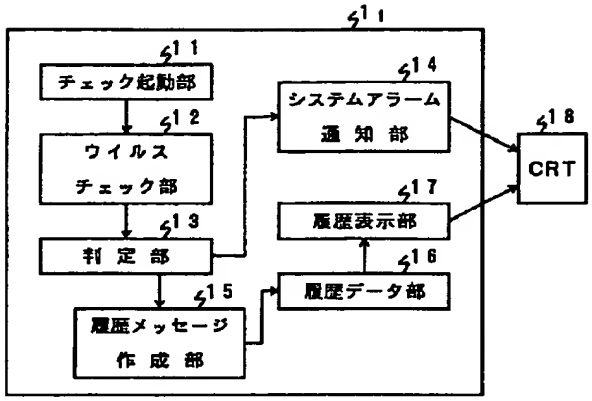
２０…ソフトウェアインストール部

Ｍ１～Ｍ４…履歴メッセージ

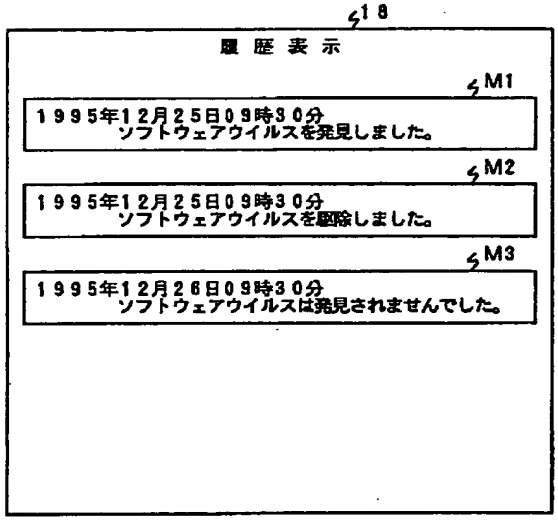
【図１】



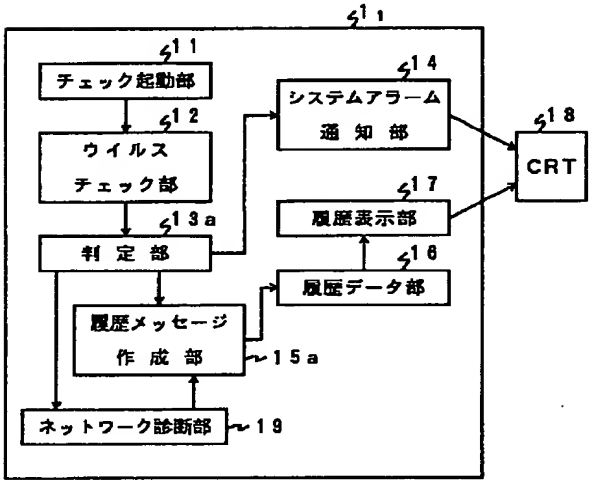
【図２】



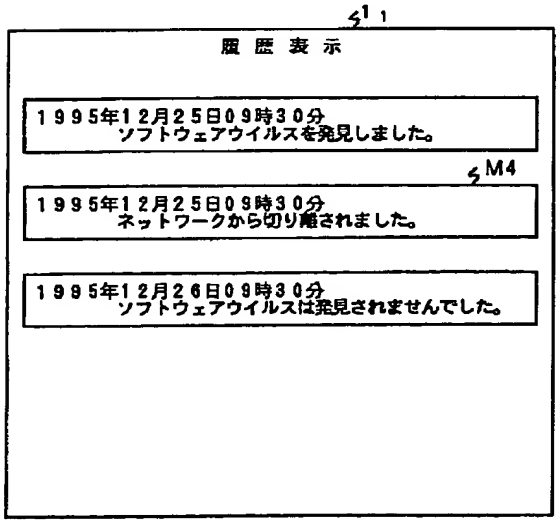
【図３】



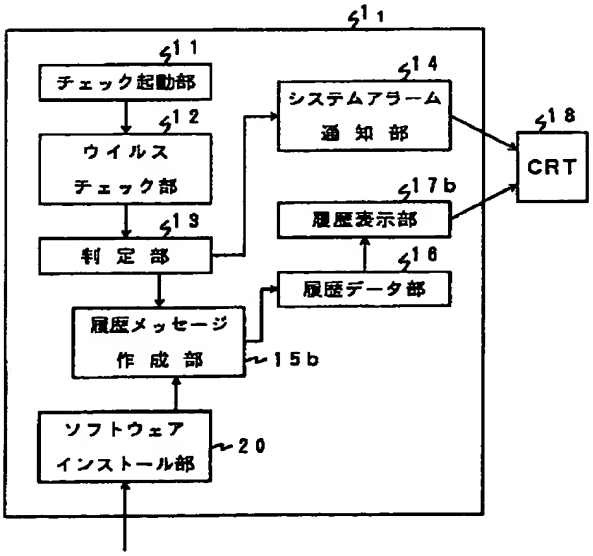
【図４】



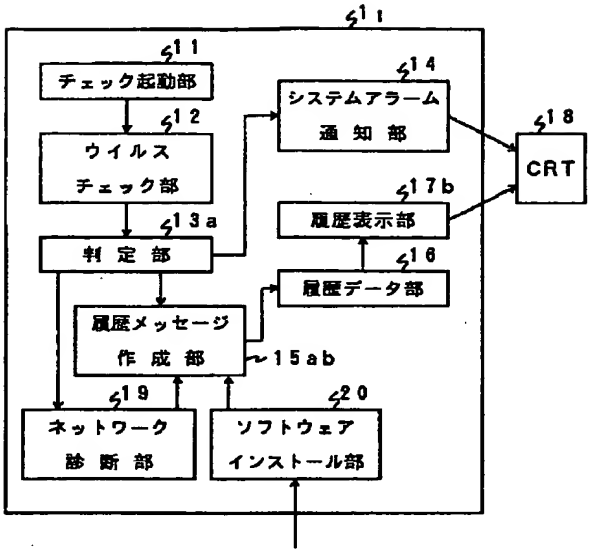
【図５】



【図６】



【図７】


11
チェック起動部
12
ウイルス
チェック部
13a
判 定 部
14
システムアラーム
通 知 部
18
CRT
17b
履歴表示部
16
履歴データ部
履歴メッセージ
作 成 部
15ab
19
ネットワーク
診 断 部
20
ソフトウェア
インストール部